Blank is confidence

In today's information overloaded world, see how once-needed data can become a threat to your organization.

"In March 2022, a travel association based in New Zealand announced it suffered a major data breach. That breach exposed the personally identifiable information (PII) of hundreds of thousands of customers collected over 15 years."

Learn how to minimize your risk caused by holding on to old data.

We are now producing hundreds of millions of terabytes of data every day. Much of this information is vital for personalizing services, predicting risks, analyzing business goals, and strategizing. While data-driven analytics are nothing new, our ability to collect quite so much information certainly is. It's useful, having all these details at our fingertips.

Until it's not. Then, that data lies forgotten, in network or drive storage environments. It becomes a ticking time bomb, waiting to create a compliance violation or data breach.

Blank is confidence because when sensitive files or folders are gone, they're gone. The information can't get into the hands of bad actors because it's not there anymore.

By contrast, when it remains behind and is not properly governed, you could face fines in the millions and an immeasurable loss of customer trust.

Information storage has become a double-edged sword for many organizations that must balance the value of data with potential liability. While many have called data a form of digital gold, two recent cases show how improper information storage and poor enterprise data erasure practices led to an expensive lawsuit and a substantial fine.

Breach exposes PII for New Zealand association's customer base

In March 2022, a travel association based in New Zealand announced it suffered a major data breach. That breach exposed the personally identifiable information (PII) of hundreds of thousands of customers collected over 15 years.

The stolen information included names, addresses, contact information, and expired credit card numbers from a division of the association that ceased operations in 2018.

Instead of deleting the no longer needed data, the association kept customer information on connected servers. If the company had followed data sanitization methods and permanently removed unnecessary information, it would have avoided this situation.

Company **executives acknowledged** this and New Zealand Acting Privacy Commissioner Liz Macpherson **agreed**.

"Companies need a review policy in place to determine if the data stored was necessary," she said, adding businesses must minimize data collection.

Collecting too much data—and not properly erasing it—provides bad actors with the opportunity to manufacture an identity.

GDPR violation brings hefty fine for Denmark financial institution

A Denmark bank was fined $1.5 million (€ 1.3 million) in the second case for failing to comply with the European Union's GDPR "right to erasure" guidelines.

GDPR requires personal data be erased by service providers when services end or legal agreements expire. Yet **key findings by the Danish Supervisory Authority** showed that the bank "has not been able to document whether rules have been laid down for deletion and storage of personal data, or whether manual deletion of personal data has been carried out."

While there was no breach, the bank held onto customer data longer than regulations allowed.

The bank faced a challenge that many organizations encounter: A distributed network of technology systems that made it difficult to build the right functionality. The organization found itself incapable of keeping up with data destruction demands in its more than 400 individual banks. Collectively, these banks process the personal data of millions of people.

See how financial institutions use Blancco: [VIDEO] Customer Testimonial: UnionBank

Why organizations keep data

Companies hold on to sensitive data for too long for many reasons:

- They may want to keep the data for future use, even if they remain unsure how that would look.
- Some firms lack data erasure software or are unfamiliar with the appropriate processes to erase data properly.
- Others believe the data will remain secure.

But keeping unnecessary data has consequences.

Retaining older data creates breach and penalty risks not worth taking

IBM's Annual Cost of a Data Breach Report shows that the average breach cost $4.35 million in 2022, up 2.6 percent from 2021 and 12.7 percent from 2020. Not only are there the costs of remediation and damage control, if a breach occurs, organizations can be held liable according to the number of records compromised.

Any unnecessary data not correctly eliminated from storage or live networks remains subject to breach. Even data stored on disconnected data center servers and decommissioned mobile devices can get accessed under certain circumstances.

In addition to breaches, GDPR infringements of certain types could result in fines. These fines can be up to €20 million, or 4 percent of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.

Instead of taking these risks, organizations need a proactive, verifiable, and certified process to permanently destroy unnecessary data.

Doing so can ensure this data is rendered inaccessible, reducing risk, maintaining customer trust, avoiding potential fines, and limiting breach exposure. Such data erasure also ensures that an organization complies with all national, regional, and market-specific regulations.

Enterprise data erasure best practices

The growth of data privacy laws will provide a framework for many organizations to manage outstanding data.

GDPR has become perhaps the most well-known, but more than 100 countries have **specific laws** that organizations should follow.

Actions you can take to minimize risk from old data:

1. **Become familiar with industry and governmental regulations** regarding data storage, protection, and deletion. Following the spirit of regulations like GDPR can serve as a solid guide. They can strengthen how enterprises protect sensitive business and consumer data. This is especially true for organizations that do not have industry-specific regulations such as **PCI DSS**, **HIPAA**, and **NCSC**, among many others.

2. **Audit your data storage.** Outside of these regulations, take a regular audit of data to determine what no longer holds value. Duplicative data, outdated customer information, information past its mandated retention date, or information related to a defunct business venture should be top contenders for data erasure. **One landmark study** shows that 85 percent of data could be obsolete.

3. **Get rid of what you don't need.** Once you determine what data is redundant, obsolete, or trivial, leverage scalable, certified data erasure methods to guarantee its permanent destruction, even across complex networks, Failing to do so can bring additional liability, risk, and stress without proper value in return.

It's important to consider not just the data in your data center or cloud environments, but also data stored on end user devices, remote and in office, particularly if staff or contractors regularly handle sensitive personal information for your customers and employees or even proprietary information your business.

By paying attention to your end-of-life data when it's no longer needed, you're one step closer to minimizing your breach risk and potential for noncompliance fines in today's regulatory environment.

The Blancco Perspective

Blank is confident, because data is truly secure when it's gone for good. Even the best, most organized enterprises can fall victim to compliance violations or data breaches when they forget about the data they don't need anymore. Regular, trackable data sanitization mitigates those threats while allowing you to enjoy the opportunities our information-heavy environment presents.

Start Prioritizing Data Sanitization

Gain confidence in your data governance practices. Learn more about the threats that unnecessary data storage presents by exploring our content hub.

Visit our content hub